

VISIT...

LANZAROTE
Caliente.COM

16

Physical Security¹

16.1	Introduction	16-1
16.2	History	16-2
16.3	Types of Intruders	16-3
	General Public • Youth Groups • Urban Gangs • Disgruntled Employees • Terrorist Groups	
16.4	Substation Development.....	16-4
	Undeveloped Property • Construction • Operational	
16.5	Security Methods.....	16-5
	Minimum Requirements • Landscaping • Fences and Walls • Locks • Barriers • Lighting • Building Design • Patrol • Signs • Clear Areas and Safety Zones • Area Maintenance • Intrusion Detection Systems • System Solutions	
16.6	Security Assessment	16-11
	Goal • Existing Station Assessment • Responsibility for Security	
	References	16-14

John Oglevie

Power Engineers

Pat Rooney

Rooney Protective Consulting Group

16.1 Introduction

Electricity is an essential service. Our society and our economy cannot function without it. It is delivered to us through the substations that we coexist with on a daily basis. Substations exist in every neighborhood of every city. They are adjacent to or within the town proper of every small town. They exist in the isolated, remote, and rural areas of most countries. More often than not, they exist next to every major commercial or industrial facility in the country. They range in size from a single transformer with fused cutouts to separate a couple of feeders, to multiple transformers in megasize stations covering tens of acres. They exist at every voltage from 2400 V to 765 kV ac and ± 600 kV dc. They are all around us. They number in the millions.

In order to provide continuous, uninterrupted service, these stations must be secured against accidental or deliberate damage to the equipment contained within. The methods used in recent times have focused on keeping the general public from harm, discouraging the vandal or neighborhood gang from practicing malicious destruction of equipment, preventing animal intrusion and subsequent contact with the energized equipment, and minimizing the liability of the owner/operator due to the injury or death of an intruder.

In the aftermath of 9-11 ([Figure 16.1](#)), attention has been focused on the threat of a terrorist attack on the electric system as a whole. There are numerous national, public, and private organizations investigating, analyzing, and publishing articles on both the strengths and weaknesses of the electric system. Individual utilities are reviewing their system integrity and security methods to determine the points of weakness within their systems and how to strengthen them.

¹Sections of this chapter reprinted with permission from IEEE Std. 1402-2000, *IEEE Guide 1402 for Electric Power Substation Physical and Electronic Security*, Copyright 2000, by IEEE. The IEEE disclaims any responsibility or liability resulting from the placement and use in the described manner.



FIGURE 16.1 A 65 MVA, 138/13 KV transformer crushed when the World Trade Center collapsed. (From ConEdison, New York, NY. With permission.)

The discussions here include a combination of the traditional methods used to provide physical security to substations as well as additional information learned since 9-11 that focuses almost exclusively on the new threat of a possible terrorist attack on a given facility. The methods discussed here can be applied to switching stations as well as substations. They are intended to include transmission and distribution stations in urban, suburban, rural, and remote locations.

Only the physical security of a station to prevent human intrusion is considered. The security for power plant switchyards is included, but not the power plant itself. Physical security for stations attached to nuclear power plants is not included, since they are generally included in the security of the plant itself. Cybernetwork security, the prevention of intrusion into a substation using electronic methods, is discussed in [Chapter 17](#), Cyber Security of Substation Control and Diagnostic Systems.

16.2 History

The earliest stations did not have security at all. The distribution system for Edison's Pearl Street station was buried in the sidewalks just under the surface. Access to the equipment could be gained just by lifting an access plate. Some of the very early hydro generating stations in the west had the distribution and switching equipment mounted on the walls adjacent to the units and without protective barriers. Prior to World War II, stations were lit by the utilities that owned them. They represented progress and were put on display. The utilities that brought electricity to town and homes were regarded with prestige. But during the 60s and 70s, with the advent of anti-establishment, anti-Vietnam war, and pro-environmental groups, the facilities became targets instead of symbols of progress. The utilities of the day had to increase the level of security around stations not only to prevent harm to individuals, but also to protect the equipment from vandalism. Now, terrorism has created yet another level of concern with the physical security of critical stations.

The events of 9-11 were not the first time utility assets have been discussed as the subject of a security threat. A panel of electric power engineers in 1950 published a report analyzing the vulnerability of domestic electric systems [1]. They stated: “The concerted attack would probably come without previous warning similar to that of the Japanese on Pearl Harbor.... Full coordination of planning activities with local, state, federal and military authorities, and adjoining electric utilities must be accomplished.”

16.3 Types of Intruders

For this document, intrusion is defined as the unauthorized human access to a substation property. The owner/operator can be a utility (either public or private), an independent power producer (IPP), or an industrial or a commercial entity in the business of generating, transmitting, or distributing electric energy. The property can be either developed or undeveloped. Intrusion can be by individuals or groups. They can be accidental, deliberate but nonspecific (vandalism), or deliberate with a premeditated purpose (malicious destruction or a terrorist act). The people or groups can be classified as follows:

- General public
- Youth groups
- Urban gangs
- Disgruntled employees
- Terrorists

16.3.1 General Public

The general public is the group that is most frequently exposed to these facilities. On a daily basis we drive by and/or work next to some portion of the transmission system. Generally we come into contact with them only by accident. Unplanned, accidental intrusion is the category of least concern. The threat to the system is minimal, while the risk to the intruder is the greatest.

16.3.2 Youth Groups

Today's community groups view stations as detractors to the value of their property, and as a result they want them to be invisible. Substation designers try to make them more acceptable by planting trees and shrubbery around them to give them an aesthetic, environmentally pleasing appearance. But hiding the station can lead the grounds to be used by youth groups as a meeting place where their actions will be hidden from the public eye. The damage these groups do to a station can be deliberate but is still random and can be classified as acts of vandalism. Types of vandalism practiced by these groups that can lead to a forced outage of the equipment can include gunshots that destroy breaker and transformer bushings, throwing chains over an energized bus, and damage to control panels in control buildings.

16.3.3 Urban Gangs

Urban gangs, unlike youth groups, are more closely associated with criminal activity. In many cases the property is not used out of convenience, as is the case with groups of youths, but as part of their territory. To indicate this they will mark their territory with the type of graffiti called “tagging.” By tagging the property, they have warned rival gangs of their claim to the property, which can lead to “turf wars” between these gangs on the property, which increases the risk of destruction to the property.

16.3.4 Disgruntled Employees

There are numerous instances on record of disgruntled employees who have caused damage within a station as the result of some grievance with the owner/operator. They pose a higher threat than youth groups or urban gangs because they represent an internal threat to the system. Their acts are not only

deliberate; they possess specialized knowledge that can be used to increase the impact to the owner/operator and to the community. There are many cases of disgruntled employees opening the oil valves on transformers. There is a case on record of a disgruntled employee attaching a homemade bomb to the side of a piece of equipment. One disgruntled employee during the 2001 Winter Olympics went into the substation control building and opened several specific breakers, which caused an area power outage of “one hour affecting 33,000 residential customers. The outage sparked a fire at the Tesoro oil refinery in North Salt Lake, which sent a plume of black smoke skyward about a mile from the Salt Lake International Airport” [2]. Disgruntled employees usually work alone. They prefer to remain anonymous. Their anger is focused solely at their employer.

16.3.5 Terrorist Groups

Terrorism is defined in the U.S. by the Code of Federal Regulations as: “the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives” (28 C.F.R. Section 0.85). EPRI has defined three types of terrorist attacks [3].

- Attacks *upon* the system: the power system itself is the primary target with ripple effect throughout the society
- Attacks *by* the system: the population is the actual target, with the power system used as a weapon
- Attacks *through* the system: utility networks provide the conduit for attacks on other critical infrastructure

There is no generally accepted definition or classification in use today with which to classify these groups. They can be grouped as either domestic or internationally based. They can be grouped into such general categories as social, political, or environmental groups; religious extremists; rogue states or state-sponsored groups; and nationalist groups. They can act for ideological, religious, or apocalyptic reasons. In today’s world, rather than being structured groups like those of the 60s and 70s, they now can be ad hoc groups that coalesce, come together for an attack, and then go away.

Regardless of the method used to classify them, they differ from all of the previous groups discussed in several ways. They are determined. They want their actions to be visible. Their intent is to interfere with some process or the completion of some project. The project can be an electric power project or some other third-party project that can be harmed through the interruption of power. These groups are organized, and their actions are planned and carefully organized. Their intent is to bring public attention to their cause; to create chaos, panic, and terror within the community; or to create a diversion as a cover for some other primary but unrelated target. They are well funded, and they have access to weapons and intelligence.

Their targets can be either symbolic or pragmatic. Symbolic targets are those that represent either directly or indirectly the actual intended target of the group. The attack on the World Trade Center and the Pentagon were symbolic because they represent the economic and military power of the U.S. Pragmatic targets are those that have a direct consequence as the result of their damage or destruction.

16.4 Substation Development

Human intrusions onto substation sites can create many problems and can occur during any of the following three stages of substation development: vacant or undeveloped property, construction of a facility, and the operational life of the station.

16.4.1 Undeveloped Property

Vacant land is most attractive to the general public, youth groups, and urban gangs. The land can be used for play, for dumping waste materials, for vandalism, and for illicit activities. With respect to play,

any number of items can draw people's attention. These include old wells, septic systems, caves, trees, rock formations, and ponds. Dumping trash can lead to civil complaints and expensive cleanup operations. The use of the property by youth groups and urban gangs can lead to public complaints and civil suits. People who are attracted to and regularly use these sites are more likely to suffer injury or death.

16.4.2 Construction

Each of the problems associated with an undeveloped property can also occur during the construction stage. In addition, there are new hazards such as excavations, uncompleted structures, and on-site construction equipment. Additional problems that can occur during construction are theft and increased vandalism. Construction materials that contain copper and aluminum are very attractive for theft. Many of these construction materials are long-lead items. Consequently theft or damage of these items can cause schedule delays. Construction equipment such as pickup trucks and excavation equipment can be stolen.

16.4.3 Operational

The operational or energized stage of the station's life does not necessarily deter people and groups from entering the facility. Incidences of vandalism and theft are just as likely to occur after a station is energized as they were in the previous two stages. But the chances of injury or death are more likely because the station is energized. Most of the groups described above lack the specific equipment knowledge to know the dangers and stay clear of energized parts. In addition, now that the station is energized, the operation or destruction of station equipment can affect the integrity of the electric power supply and the reliability of the transmission and distribution grid, if the intrusion results in power interruptions. Intruders have been known to open valves, push buttons, and operate circuit breakers, reclosers, and switches.

16.5 Security Methods

Security requirements should be identified in the early design stages of the substation project. Generally, it may be more economical to anticipate and incorporate security measures into the initial design rather than retrofit substations at a later date.

16.5.1 Minimum Requirements

The minimum security requirement for every station is to prevent injury or death of someone by coming into contact with energized equipment. The best way to do this is to prevent the site from being used as a gathering place for individuals and groups and to prevent entry to the station by unauthorized and untrained individuals. Fences of varying kinds, walls, locks, lighting, landscaping, and control-building design are all methods employed to keep both trained and untrained persons from harming themselves. Beyond this basic need, other security methods have been developed to detect or prevent unintended or unlawful entry onto a site. These include motion detectors, video cameras, guards, SCADA-monitored doors and locks, and enhanced building security systems. The level of security appropriate to a given station will be discussed in Section 16.6 of this chapter, Security Assessment.

16.5.2 Landscaping

Landscaping around a substation can make the station more pleasing to the surrounding community, but the landscaping should be carefully designed so as not to create hidden areas that are attractive as a meeting place for people and groups. Landscaping must be regularly maintained. Trees and shrubbery must be pruned to avoid concealing intrusion and illegal activity. An appearance of "pride in ownership" can project an image of regular visits by personnel that will keep many would-be intruders away from the facility.

Consider using thorny plants or bushes near fences and walls to deter potential intruders from tampering with physical barriers. Plants such as firethorn (*pyracantha*), barberry (*berberis*), quince (*chaenomeles*), yucca, rose bushes, and certain types of holly are good examples of plants that can be used to deter intruders. Avoid plants that may interweave through fencing fabric.

16.5.3 Fences and Walls

Every station has a perimeter fence around that portion of the property used for the energized equipment. It is the first line of defense against intrusion. Fences are also used inside the station proper to provide an additional safety barrier for trained personnel working in the yard.

Fences of various materials can be used to provide primary security to limit access to substation property. Refer to the National Electric Safety Code (NESC) (Accredited Standards Committee C2-2002) for fence requirements. In addition, there are numerous IEEE standards and guides detailing the fencing requirements for various applications such as shunt and series capacitor banks, shunt reactors, etc.

Fences can be either fabric or solid walls. Fabric fences will stop the casual intruder from entering the station yard. They are usually chain link with three strands of barbed wire at the top to discourage an intruder from climbing the fence to gain entry. The designer should keep in mind when considering a fabric fence that the stronger and more difficult the fence is to breach, the more determined the individual or group must be to gain entry to the station.

In general, consider using a commercial-grade, galvanized fabric, either 3.0 mm (11 gage) or 3.8 mm (9 gage). The mesh opening size should preferably be 50 mm (2 in.), but not larger than 60 mm (2.4 in.) to resist climbing. The height of the fence should be a minimum of 2.1 m (7 ft) above ground line. In cold areas, it is preferable if the fence is 2.1 m (7 ft) above the maximum snow accumulation. In higher risk areas, consider using three strands of razor wire, angled toward the outside away from the facility. Areas vulnerable to vehicle penetration may consider reinforcing the fence with 19-mm diameter (or larger) aircraft cable mounted to the fence supports, inside the mesh fabric, at a height of approximately 0.75 m (30 in.) above ground level.

Solid walls can be either masonry or metal. Solid walls have the advantage of preventing direct line-of-site access to equipment inside the station. Solid walls may prevent external vandalism such as gunshot damage.

16.5.4 Locks

All entrances to substation sites should be locked. Control buildings should have locked metal doors. All equipment located outdoors within the substation fence should have a provision for locking control cabinets, and operating handles should be padlocked. Padlocks should be true high-security locks, as recognized by Underwriters Laboratories, using restricted-duplication keys.

It is strongly recommended that a key-control program be adopted by the owner/operator to control the distribution of all keys. Each person in possession of a key should be accountable for the location and control of the keys at all times. All keys should be logged, indicating who has the key, to what the key gives them access, the date the key was issued and returned, and for what reason the key was returned. This log can provide crucial information in the case of an intrusion by a disgruntled employee. The log will also help determine if and when locks or cylinders should be changed.

16.5.5 Barriers

Access to energized equipment and bus may be of concern if the perimeter security measures are breached. Polycarbonate or other barriers on access ladders and structure legs can be used to provide additional barriers to access. Refer to NESC and Occupational Safety and Health Administration (OSHA) requirements. Driveway barriers (gates, guard rails, ditches, etc.) at the property line for long driveways can help limit unauthorized vehicular access to the substation property.

All sewer and storm drains that are located inside the substation perimeter, with access from the outside, should be spiked or fitted with vertical grillwork to prevent entry. Manhole covers or openings should be located on the inside of the substation perimeter fence.

16.5.6 Lighting

The entire interior of the substation could be illuminated with dusk-to-dawn lighting that provides a minimum light level of 21.52 lx (2 fc). However, some caution is necessary here. Local residents may complain about this level of lighting at night, or local zoning ordinances may restrict or prohibit lighting altogether. Do not use sodium vapor lighting if the lighting is intended to assist with the identification of intruders or is to be used in conjunction with video scanning equipment. This type of light or any lighting fixture that produces a yellow or orange cast will interfere with attempts to identify the person, his clothing, and the description of the person's vehicle.

All wiring to the lighting posts should be in conduit or concealed to minimize tampering by an intruder. Areas outside the substation, but within the facility property, should also be considered for lighting to deter loitering.

16.5.7 Building Design

In general, most building materials provide adequate security protection. Selection of the type of building construction should be suitable for the level of security risk. Typically, features that should be included are steel doors with tamper-proof hinges and roof-mounted heating/air-conditioning units. Any wall openings (i.e., wall air conditioners) should have security bars over and around the unit. A building that is part of the perimeter fence line should be at least as secure as the fence. Construction of a building to enclose the substation or exposed equipment and materials can provide an additional layer of protection against intruders. For example, using trailers or buildings to enclose material stored at construction sites may deter theft.

16.5.8 Patrol

In areas where vandalism has been a chronic problem and at critical substations, judicious use of security patrol services could be considered. A partnership should be established with local law-enforcement agencies to facilitate the need for local patrols of selected substation facilities to deter vandalism and unauthorized entry. Security procedures should be established that specifically identify who handles security alarms and what the notification procedure is within the company and local law-enforcement agencies. Furthermore, during special or unusual occasions within the area of the station — e.g., labor disputes, the Olympics, or visits by heads of state — security procedures at critical substations may include identification checks by security patrols and limited access to the substation.

During a disaster, responding security or law-enforcement personnel may not be able to respond within an acceptable time due to transportation restrictions or higher priority emergencies. However, proper planning for disasters that might occur in a given location can help to protect a substation and preclude the need to deploy personnel during the event. Failure to recognize the impact of the following events and to institute precautions could result in numerous false alarms:

- Wind: Do not use security measures that might be activated by high winds.
- Animal: Numerous methods and products are available to assist with minimizing animal intrusion and reducing false alarms. Various methods and their effectiveness are discussed in IEEE Std. 1264-1993, Guide for Animal Deterrents for Electric Power Supply Substations.
- Seismic activity: Do not use devices that could be triggered by earth tremors.
- Vehicular, rail, or aircraft intrusion: While prudent siting methods can reduce the likelihood of such an event, substations at times must be contiguous to these modes of transportation as a matter of necessity. Alternative means of accessing the site can be helpful when the normal access is blocked by an intrusion. In addition, prudent planning for emergency response to the above should include the availability of items such as emergency lighting and temporary fencing materials.

16.5.9 Signs

Signs should be installed on the perimeter fence to warn the public that:

- Alarm systems are providing security for the substation.
- Entry is not permitted.
- There is a danger of shock inside.

Include a sign with the station's location address and an emergency phone contact number.

16.5.10 Clear Areas and Safety Zones

Structures and poles should be kept a sufficient distance from the fence perimeter to minimize the potential use of the structure itself to scale the fence. Where practical, establish a 6-m (20 ft) to 9-m (30 ft) clear zone around the exterior of the perimeter fence. The clear zone will provide a clear field of view, making it easier to detect someone attempting to enter the facility illegally. Similarly, a double row of area fencing (enclaving) could be used to set up a clear zone inside the station to increase the difficulty of accessing the energized portions of the station.

16.5.11 Area Maintenance

The owner/operator should provide frequent and routine inspection of the station property. Maintaining the station property in a clean and orderly fashion establishes a level of care that the area is regularly patrolled, thus helping to discourage various groups from using the property as a meeting place. A regular preventive maintenance program should be developed to have security measures inspected regularly and deficiencies rectified before they lead to security problems.

Tagging by gangs requires special attention. Tagging may well indicate a heightened use of the property and should be dealt with immediately by working with law enforcement to identify the group and increase the physical security of the station. It is strongly recommended that tagging be removed as soon as local law-enforcement officials document it.

16.5.12 Intrusion Detection Systems

Numerous systems are now on the market to detect unlawful entry to a station. Sophisticated motion detection systems, video camera surveillance equipment, and building security systems are becoming more common. All of these systems are designed to provide early detection of an intruder so that law-enforcement personnel can be dispatched to the site to investigate.

Perimeter systems using photoelectric or laser sensing can be utilized to provide perimeter security. Overall motion-sensing devices may provide area security; but animals can trip these devices, which over time could render these devices ineffective.

Video systems can be deployed to monitor the perimeter of the substation, the entire substation area, or building interiors. They can have zoom lenses added to allow the reading of gauges located in the yard. They can be programmed to move to a specific combination of angle and zoom to provide a clear reading of a level or temperature gauge. They can also be moved to view any specific area of the station yard where illegal entry is suspected. Video systems are available that use microwave and infrared to activate a slow-scan video camera that can be alarmed and monitored remotely and automatically set to videotape the scene.

One of the more common methods used is an intrusion alarm on the control building door. These systems include, at a minimum, magnetic contacts on all the doors and have provisions to communicate to the operations center through the existing telephone network or SCADA system. They can also include a local siren or strobe light located on the outside of the building that is activated under an alarm condition. The systems should be capable of being activated or deactivated using an alphanumeric keypad, keyed switch, or card reader system located inside the building. All siren boxes and telephone connections should have contacts to initiate an alarm if they are tampered with.

TABLE 16.1 Effectiveness of Security Methods — Urban Substations

Method	Number of Respondents Reporting to Survey	Respondents Reporting Method Not Effective (%)	Respondents Reporting Method Somewhat Effective to Effective (%)	Respondents Reporting Method Very Effective to Completely Effective (%)
Lights	31	7	77	16
Signs	27	7	78	15
Special locks	18	1	66	33
Solid wall	7	0	57	43
Security guard	5	0	60	40
Manned station	4	0	100	0
Optical alarms	4	0	75	25
Fence	4	0	75	25
Video camera	3	0	100	0
Special equipment (metal-clad, polymer)	3	0	67	33
Door alarm (to SCADA)	2	0	0	50
Alarm system	2	0	0	100
Motion detectors	1	0	0	100
Electronic protection	1	0	0	100

TABLE 16.2 Effectiveness of Security Methods — Suburban Substations

Method	Number of Respondents Reporting to Survey	Respondents Reporting Method Not Effective (%)	Respondents Reporting Method Somewhat Effective to Effective (%)	Respondents Reporting Method Very Effective to Completely Effective (%)
Lights	31	6	78	16
Signs	27	11	81	8
Special locks	19	5	69	26
Security guard	6	0	100	0
Fence	5	0	60	40
Solid wall	4	0	75	50
Manned station	4	0	100	0
Optical alarms	4	0	100	0
Video camera	3	0	100	0
Special equipment (metal-clad, polymer)	3	0	67	33
Door alarm (to SCADA)	2	0	0	100
Alarm system	2	0	0	100
Electronic protection	2	0	0	100
Motion detectors	1	0	0	100

Both IEEE and CIGRE have issued survey forms to their membership requesting data to determine the effectiveness of each type of security system. The CIGRE report is yet to be published. The results of the IEEE survey, first published in 1999, are shown here as Table 16.1 through [Table 16.4](#).

16.5.13 System Solutions

The more sophisticated the security system, the more determined and organized the intruder has to be to gain entry. Tables 16.1 to 16.4 indicate that some security measures are much more effective than others, but none of them are 100% effective either singly or working in combination with one another, especially when an organized, well-trained, and determined terrorist group is considered. Under these

TABLE 16.3 Effectiveness of Security Methods — Rural Substations

Method	Number of Respondents Reporting to Survey	Respondents Reporting Method Not Effective (%)	Respondents Reporting Method Somewhat Effective to Effective (%)	Respondents Reporting Method Very Effective to Completely Effective (%)
Lights	31	13	74	13
Signs	22	11	77	12
Special locks	17	6	65	29
Optical alarms	5	0	100	0
Fence	5	0	60	40
Passive and microwave systems	4	0	0	100
Security guard	4	25	50	25
Video camera	3	0	66	34
Manned station	3	0	100	0
Special equipment (metal-clad, polymer)	3	0	100	0
Alarm system	2	0	0	100
Door alarm (to SCADA)	1	0	0	100
Solid wall	1	0	100	0
Motion detectors	1	0	0	100
Electronic protection	1	0	0	100

TABLE 16.4 Effectiveness of Security Methods — Industrial/Commercial Substations

Method	Number of Respondents Reporting to Survey	Respondents Reporting Method Not Effective (%)	Respondents Reporting Method Somewhat Effective to Effective (%)	Respondents Reporting Method Very Effective to Completely Effective (%)
Lights	28	4	82	14
Signs	25	8	84	8
Special locks	15	7	73	20
Security guard	5	0	40	60
Solid wall	3	0	34	66
Manned station	3	0	100	0
Fence	3	0	66	34
Video camera	2	0	100	0
Optical alarms	2	0	100	0
Special equipment (metal-clad, polymer)	2	0	50	50
Door alarm (to SCADA)	1	0	0	100
Alarm system	1	0	0	100

circumstances and in the aftermath of 9-11, security measures must be refocused. The security of a substation must be viewed in the larger context of the security of the overall electric system. One approach is to “improve the security of the nation’s power systems not by building fortresses around large, fragile facilities ... but by strategically evolving a more resilient electric network.” This is a network that “is designed not to make component failures impossible but to permit failures to occur without catastrophic effects on the essential functions of the system” [4].

To provide greater security to the system as a whole, utilities are looking at the following criteria.

- Building a redundant network. The transmission system should remain stable during the outage of any two lines or substations anywhere in the system. This is a double-contingency (N-2) planning criterion.
- Maintaining spares for critical hard-to-replace pieces of equipment. This can include transformers, breakers, and even station structures.
- Earmarking spare equipment that is critical to the region and entering into agreements with other utilities in the region as to the storage, availability, and use of the equipment.
- Designing station yards to include wide internal roadways that provide easy access for mobile transformer equipment. Provide attachment points to minimize the time required to restore partial power to critical loads.
- Using underground feeders for critical loads.
- Using comparable design standards with neighboring utilities. The use of similar design standards will allow easier sharing of common equipment during emergencies.
- Locating distributed generation resources near critical loads or near critical stations that do not meet the N-2 double-contingency criteria.
- Placing new stations indoors using gas-insulated equipment and underground feeders.
- Considering alternative bus designs that provide higher levels of line protection and source-load redundancy.
- Spacing equipment farther apart to prevent collateral damage.

16.6 Security Assessment

16.6.1 Goal

The level of security to be applied at any station requires an assessment of the station's importance within the system and the type of intruder(s) that might pose a threat to the security of the station. The objective of any security system assessment program and implementation policy is to achieve the following:

- Determine what makes the station attractive and a potential target for damage.
- Mitigate or remove entirely the attractiveness.

Consider the following factors when determining the importance of each existing or new station in the system:

- Does the station serve critical or sensitive load such as local emergency services, military installations, or major industries?
- Is the station designed to provide double-contingency protection for all critical loads and lines?
- Does critical load served by this station have alternative sources of power available during emergencies?
- Will loss of this equipment cause area-wide voltage- or frequency-stability problems?
- What is the maximum length of time required to restore or replace damaged critical equipment in this station? Is this length of time acceptable? Can the customer tolerate loss of power for this length of time?

16.6.2 Existing Station Assessment

A great deal of information about the attractiveness of stations within the system can be determined from the service history of the existing stations. The designer can then use this knowledge when considering the appropriate level of security for a new station.

The security assessment form reproduced here ([Figure 16.2](#)) first appeared in IEEE Guide 1402 and can be used for assessing the security of each existing system station. Its importance cannot be stressed

Security Assessment

Assessment completed by: _____

Date: _____

I. SUBSTATION LOCATION: _____

II. SUBSTATION CLASSIFICATION:

A. Type:

- | | | |
|--|--|---|
| ☐ Rural | ☐ New facility | ☐ Permanent facility |
| ☐ Urban | ☐ Existing facility | ☐ Temporary facility |
| ☐ Construction site | | ☐ Land bank |

1. Construction type _____
2. Location _____
3. Distance to nearest occupied facility _____
4. Type of access road _____
5. Visibility/screening from view _____
6. Distance to regularly traveled road _____
7. Topography _____
8. Environmental consideration _____

B. Planned activity:

- | | |
|---|---------------------------------------|
| ☐ Vacant | ☐ Construction |
| ☐ Pre-construction | ☐ Operational |

C. Equipment involved:

- | | |
|--|---|
| ☐ None (unoccupied) | ☐ Construction equipment |
| ☐ Storage | ☐ Energized facility |

III. SITE RISK EVALUATION:

- | | |
|--|-----------------------------------|
| Local demography | Labor conflicts/disputes |
| Local economics | Adjacent landowners (uninhabited) |
| Local crime rate/reported incidents | Adjacent landowners (inhabited) |
| Local building/construction aesthetics | Substation value |

IV. SITE MAINTENANCE:

	Yes	No
A. <u>General observation:</u>		
Evidence of use	☐	☐
Bottles and/or cans	☐	☐
Refuse	☐	☐
Standing water	☐	☐

Comments/explanation: _____

FIGURE 16.2 Security assessment form.

	Yes	No
B. <u>Walls and fences:</u>		
Damage	☐	☐
Graffiti	☐	☐
Broken strands or holes	☐	☐
Rust to galvanizing	☐	☐
Undermining	☐	☐
Evidence of attempted entry	☐	☐
Damage to locks or hinges	☐	☐
Comments/explanation: _____		

	Yes	No
C. <u>Station yard:</u>		
Refuse	☐	☐
Disturbed grading	☐	☐
Damage to grounding conductor or hardware	☐	☐
Graffiti on walls or equipment	☐	☐
Loose valves or evidence of tampering	☐	☐
Evidence of vandalism	☐	☐
Broken or chipped porcelain	☐	☐
Comments/explanation: _____		

	Yes	No
D. <u>Control building:</u>		
Attempted entry	☐	☐
Stolen or missing maintenance equipment	☐	☐
Evidence of occupancy	☐	☐
Tampered control equipment	☐	☐
Comments/explanation: _____		

Comments/other: _____		

Recommendations: _____		

FIGURE 16.2 (Continued)

enough as part of an organized security policy. A plan for evaluating the effectiveness of any mitigating measures should be initiated. A history record should be kept for each substation to document the security option used, the problem the option is intended to mitigate, and the date of application. In addition, a record of the type of intrusions will help the designer evaluate the effectiveness of the security options chosen and identify weaknesses or shortcuts that an intruder has used to advantage. The record can also be used to evaluate the feasibility of future applications.

16.6.3 Responsibility for Security

Identification of the person or persons responsible for security implementation and administration is critical to the effectiveness of the plan. Defined levels of responsibility and specific tasks are required for each level. Each company should have one person in charge of facilities security. This individual should be responsible for assuring that a security plan is developed, implemented, regularly reviewed, and updated. Regular inspection of facilities to assure that security measures are in effect should be part of the security plan. Employee training and methods that enable employees to report irregularities or breaches of security should be instituted.

References

1. Badolato, E., Physical Security of Electric Power Systems, CMS, 2001; www.CMSINC.freesevers.com/physicalsecurityforelectricpowersystems.pdf.
2. Cantera, K., Inquiry Narrows in Games Blast, *Salt Lake Tribune*, Sep. 20, 2002.
3. Gehl, S., Electricity Infrastructure Security, Power Point presentation, EPRI, Palo Alto, CA, Nov. 28, 2001.
4. Regulatory Assistance Project, Electrical Energy Security: Policies for a Resilient Network, Part II, Gardiner, ME, Apr. 2002; www.rapmaine.org.